heart of the south west
Growth Hub

BUSINESS GUIDE
Bring Your Own Device (BOYD)

Bring Your Own Device

By Barnaby Page

BYOD, or 'Bring Your Own Device', describes the increasingly common practice of organisations actively allowing employees to use their own smartphones, tablets, laptops and the like for work.

We say 'actively allowing', because what's new about BYOD is not that individuals within the workforce are bringing their own equipment to the office or working with it off-site - which of course has happened for many years - but that managements and IT departments are now seeking to formally recognise that employee-owned equipment is part of the business's technology landscape.

The term BYOD probably derives from the use of BYOB, or 'bring your own bottle', on party invitations - but the resemblance stops there, because BYOD is a serious issue which poses potential management, cost, and above all security challenges.

On the other hand, it can make for a more flexible and effective workforce, and there is also a strong argument that since staff are inevitably going to use their own devices for work *anyway*, it is better to manage them than to ignore them.

In short, formulating and implementing BYOD policy is all about balancing freedom of choice with security and manageability.

However, acceptance of BYOD is far from universal. Some organisations are opting for an alternative model sometimes called COPE, for 'Corporately-Owned, Personally-Enabled', or CYOD, for 'Choose Your Own Device'. In essence, this involves the organisation supplying staff with devices for their own use and allowing them some say in what models they have, but retaining ultimate ownership and control. This is a real, but very different, alternative to BYOD.

BYOD does not have to be an all-or-nothing approach. While it sometimes completely replaces corporate-owned devices, especially for contractors, it frequently co-exists with them in the same organisation.

Every month about half of people with a personal smartphone use it for work email, and a similar percentage access work files or data (source: Azzurri/Shape the Future)

Scope and Development of BOYD

In the typical organisation, BYOD began with senior executives using their own laptops, mobiles and suchlike on an informal basis, as early as the 1990s. Since then, staff at all levels have become much more digitally-enabled in their personal lives, and so the practice has spread.

The increasing ubiquity of wireless connections has also contributed to its growth, as has the much greater computing power of modern smartphones compared to older mobiles, enabling them to run applications that were previously confined to the desktop or laptop.

Email is generally considered the 'killer app' most beneficial to BYOD users, while calendar applications are also widely appreciated. Voice calls and text messaging are also popular uses of BYOD phones for business, while email is more dominant on tablets.

Today, the departments which have the most to benefit from BYOD usually include sales, marketing, IT, and customer services. However, BYOD policies tend to encompass all staff, rather than allow more or less usage in any particular department.

The term BYOD does not have a narrow definition. While everyone agrees it covers smartphones, laptops and tablets, others extend it to equipment which workers do not literally 'bring' anywhere - for example their home PCs - and even to applications which they install on their own initiative, or online services which they subscribe to. In all these cases, the key is that the decision on what to use has been taken by the employee, not the business.

Pros and Cons of BOYD

Flexibility and productivity

BYOD gives employees the flexibility to work where and when they need to. As with other forms of flexible working (such as teleworking), this tends to improve productivity and lead to increased working hours. For example, commuting time can be used to deal with email on a personal device.

It's true that this flexibility could also, in theory, be achieved by issuing company-owned equipment. But in practice few people will carry a company laptop with them unless they have to, while most of us are in possession of our smartphones - or even tablets - all day. The sheer ease of working on a familiar, always-on device rather than having to dig out and power up a work-specific device is one of the biggest drivers for the adoption of BYOD.

An increase in the total number of hours worked is not the whole benefit, however. Flexibility in *when* they are worked can be just as important. For example, someone awaiting an important email from a distant time zone can, if their personal device is enabled to handle work email, deal with it as soon as it arrives rather than waiting until the next morning.

Of course, as with any form of flexible working, it's important to ensure that the flexibility employees now have to work outside the office location and hours doesn't turn into pressure for them to be available 24/7.

Cost implications

The cost implications of BYOD are not clear-cut, and estimates vary to the amount that employers will save on both not having to buy equipment, and spend on supporting and making secure a wider variety of employee-owned devices.

One estimated figure that at least offers a rule of thumb is that it will cost an average of just over £90 per employee 'to implement a policy which allows the same mobile device to be safely used for both private and business use' (source: Azzurri/Shape the Future). Other sources suggest a lower sum, however.

In any case, the following factors should be considered when projecting the costs of implementing a BYOD policy:

- Costs of voice and data. Even if the employee is meeting the bill it is usual for employers to provide some subsidy toward it. Employees may not be on the most cost-effective plans, and the employer will not benefit from bulk contracts
- IT, support and help desk costs. There will almost certainly be upfront IT costs in making the business's systems available on personal devices, and in making those devices secure. These could include costs of developing new software, and of buying in mobile device management (MDM) software. There are also likely to be continuing costs in providing support when users have difficulty using their personal devices with business systems, and there is a risk that this could spill over into providing support for use of the devices in general
- Costs of purchasing a device, in a COPE/CYOD situation - these clearly don't apply with BYOD

Against all these should be set the tangible gains of BYOD in not having to purchase equipment, and the less tangible but very real gains of a more productive workforce.

Security

Although costs are important, they are unlikely to be the make-or-break factor in a business's decision on whether, or how far, to introduce BYOD. Security is the number one concern, and the risks are manifold.

Personal devices are, by their nature, unlikely to be as well-protected as a corporate network - placing commercially sensitive data and intellectual property at risk, as well as raising the spectre of breaches of the law in areas such as data protection.

They can also bypass content filtering systems, both inbound and outbound, allowing malware and other digital undesirables to enter the company network or indeed leave it; and they can be used to access highly insecure websites and other online services.

Because they are carried around all day, they are more liable to loss or theft than equipment that stays at the office. And, of course, when an employee leaves the business, the device - and potentially all the data stored on it - leaves with them.

These concerns are genuine but they are not insurmountable. In the section *Managing BYOD Security* below, we look at some of the measures that can be taken to ensure the security of BYOD devices, and enjoy the benefits of BYOD at minimal risk.

Practical Management of BOYD

Establishing and implementing a BYOD policy

As we have noted, BYOD has been happening informally in many organisations for some time. But now a number of factors - including its increasing adoption at all levels, and the growing ability of smartphones, tablets and other personal devices to handle full-blown business applications as well as making calls and sending texts - mean that a formal BYOD policy is becoming necessary to manage risk and bring order to chaos.

Input on formulating a policy will be needed from departments including IT, Finance, HR, and Legal, and listening to their concerns will help develop support for BYOD. While downsides cannot be ignored, it is important that BYOD is seen as ultimately a benefit rather than a liability to the organisation.

Elements of a policy should include:

- Eligibility - who can use BYOD? (Normally, once it's formalised, any employee who could benefit from it is entitled to take advantage of BYOD.) What devices are supported? (This need not be a list of models - it might just specify what kinds of devices are allowed, and minimum features. Currently, support for Windows and iOS is considered a priority by most businesses, with Android and BlackBerry less important.)
- Technology - how are applications and data normally held on the business's own network made available to personal devices? Where are they stored? How are updates and upgrades handled? What additional software, for example anti-virus, will be required on the employee's device - and who will pay for, and manage this? Remember that changes in the technology of personal devices, as well as changes in the business's own IT systems, might mean continual adjustments to the interface between them
- Support - what aspects of the personal device and its use will the business support, in terms of providing assistance to users? What about support on issues such as connection to home or third-party Wi-Fi networks? A line must be drawn somewhere
- Usage - if the same device is being used personally and for work, it's important to keep those uses distinct. For example, employees shouldn't send private emails from a work address, even if it's accessible on their own phone
- Cost bearing - what will the business pay for? How will costs be tracked? Are there implications for software licences?
- Rollout - will BYOD be implemented for all users, all applications, all data, and all devices simultaneously, or will it be easier to introduce it progressively? Will training be required?
- Security - discussed in the section below

Managing BYOD Security

The simplest approach to BYOD security is not to allow BYOD at all, but as we have seen, in the majority of organisations this is a vain hope.

Instead, the focus of most advice is to *control data and not the device*.

One simple philosophy is to assign different levels of security to data and applications, such as:

- Most secure level - must not be used on BYOD devices at all, for confidentiality or legal reasons
- Medium security level - can only be accessed through terminal sessions, where the employee's device can log on to the business's servers, but doesn't run application software or hold data
- Minimum security level - can be used and stored on BYOD devices

Mobile device management (MDM) software is an important tool, allowing the business to remotely manage the devices that are accessing its network, and prevent them from using its systems if their security is inadequate. For example, MDM can ensure that passwords and encryption protect applications and data, and remotely wipe information if an employee leaves the business or loses the device.

User profiles can also be devised to limit the kinds of data, applications and activity that individual employees are permitted with their personal devices.

All these tactics focus on data rather than hardware. However, security can also call for limitations on the specific devices that employees are permitted to use - for example, forbidding those that are jail-broken (i.e. with a hacked operating system), or won't work with mobile device management (MDM) software.

Further Information

Web Resources

GCHQ's CESG has numerous recommendations on security for BYOD:
https://www.gov.uk/government/collections/end-user-devices-security-guidance--2

The Information Commissioner's Office advises on data protection and BYOD:
http://www.ico.org.uk/for_organisations/data_protection/topic_guides/online/byod

A model policy on BYOD security:
http://www.iso27001security.com/ISO27k_Model_policy_on_BYOD_security.pdf

Some major MDM software suppliers:
http://www.business-software.com/offer/top-10-mobile-device-management-software/

heart of the south west Growth Hub

Top Tips

Embrace BYOD
Don't try to ban BYOD - manage it instead.

Ensure you have support for any BYOD initiative
Get buy-in from all departments by listening to their needs and concerns.

Focus on usage and data, not devices
You efforts should concentrate on how the devices are being used and the ways in which any sensitive or confidential data they may hold will be protected, rather than simply the devices themselves.

Put a framework in place
Don't be afraid to make rules. BYOD doesn't have to be a free-for-all.

Implement appropriate levels of security
But don’t be so secure that users become frustrated, or seek ways around the security.

Make sure that applications are the driving force
Avoid altering the functionality of applications just so they'll work on personal devices.

Remember that different users will have different preferences
Don't make BYOD policy dependent on a specific mobile operating system.

Plan for the future as well as the present
Remember that technology changes fast - connecting business systems to BYOD devices is not a one-off job.

It’s not about the cost savings
Don't expect to save a lot of money - the benefits are more about effective and flexible working.

heart of the south west local enterprise partnership

Department for Business Innovation & Skills

The Heart of the South West Growth Hub Service

The Heart of the South West Growth Hub provides the key access point for business support in the Heart of the South West LEP area; Devon, Somerset, Plymouth and Torbay. We deliver independent diagnosis and referrals to existing business support services.

The Growth Hub service is the first point of contact for both new and established businesses seeking business support; the Growth Hub team is on hand to answer questions or make referrals to experts in specialist areas such as funding opportunities, tax advice, exporting or innovation.

The Growth Hub provides access to all local and national business support services and is offered completely free at point of access for all businesses seeking advice. The Growth Hub can help any business sector and any business size.

The Growth Hub is the Heart of the South West Local Enterprise Partnership's main mechanism of engaging with businesses across the area.

Service Components

Online Business Advisers – our experienced team will talk through your business goals with you and put you in touch with the best support to help you achieve them

Outreach Events – we will be running events and workshops across the Heart of the South West LEP area where you can speak to our Online Business Advisers

Website – our web portal will provide access to information about all the business support currently available in your local area as well as links to national programs. You will also find full listings of local business support events.

Information Provision – our monthly e-newsletters provide updates on support services available to businesses such as advice, grants, funding, events and workshops and key business topics such as sales, marketing or public procurement opportunities.

General enquiries	info@heartofswgrowthhub.co.uk
Telephone	**03456 047 047**
Website (interim)	www.heartofswgrowthhub.co.uk
Sign up for e-news	www.heartofswgrowthhub.co.uk/newsletter-subscription